IV&V Role ESSP AO Process

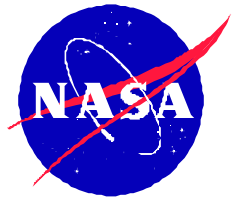
Kenneth A. Costello, IV&V Project Development Lead

NASA Software IV&V Facility

NPD 8730.4 for Software Independent Verification and Validation (IV&V) Policy states: "…task the IV&V Facility in Fairmont, West Virginia to manage the performance of all IV&V for software identified per the established criteria, and for any other safety critical software (as defined in NASA-STD-8719.13A)."

www.ivv.nasa.gov
GSFC, Code 307
Director: Nelson Keeler

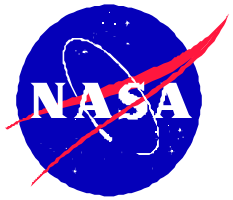
NASA IV&V Policy (NPD 8730.4)



NASA will:

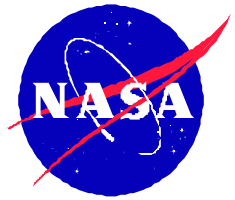
- Establish and apply a criterion, tools, and methodology to evaluate and assess software risk to identify appropriate level of IV&V
- Task the NASA IV&V Facility in Fairmont, WV, to manage the performance of all IV&V for software in Provide Aerospace Products and Capabilities (PAPAC) programs and projects identified per the above criterion and any other safety critical software (as defined in NASA-STD-8719.13A)
- Require PAPAC programs and projects to determine the level of IV&V to be performed with the explicit involvement of the IV&V Facility
- Require NASA programs and projects that contain mission or safety critical software to document decisions concerning the use of IV&V

What is IV&V?



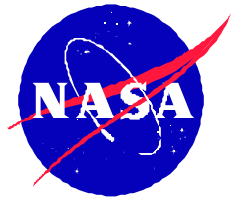
- Software IV&V is a systems engineering process employing rigorous methodologies for evaluating the correctness and quality of the software product throughout the software life cycle
- Make a Value-added Contribution, Everyone Shares the Similar Objective of MISSION SUCCESS
  - For PM – Provides objective view of the software development effort
  - For Everyone Else – Provides unbiased source of help
- As a Partner on the NASA Team, Helps Deliver
  - Risk Identification and Mitigation Technique
  - Increased Quality and Safety
  - Improved Timeliness and Reliability
  - Reduced Cost
- IV&V works closely with the developers
  - The formal interface will be with an IV&V Facility project manager
  - Informal interface between the IV&V analysts and the developers
  - Helps to get identified problems and issues into the appropriate hands quickly
- Results of the effort will be documented
  - Issues will be identified to the developers in a timely manner
  - Status reports to the project management

Independent Analysis



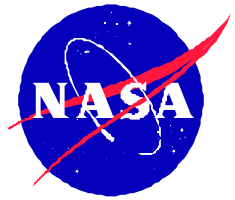
- Independent Verification and Validation
  - Defined as verification and validation performed by an organization that is technically, managerially, and financially independent of the development organization [IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology]
  - Further defined as the application of the IV&V Facility processes in support of a decision to deploy the program/project being developed
  - This includes software life cycle analysis appropriate to the criticality and risk associated with the software within the context of all the program/project's mission and goals
  - IV&V reflects a continual function across the life cycle of the project to assure mission requirements and system design changes are correctly carried forward across the software life cycle phases and organizational transitions (e.g. NASA to contractor and vice versa)
  - When IV&V is performed, the resulting tasks are based on the cost, size, complexity, life span, risk and consequences of failure of the software within the context of the program/project's mission and goals
- Independent assessment differs in scope from an IV&V effort
  - A subset of the IV&V analysis is applied to particularly critical software components or processes
  - This analysis can be performed as a one-time effort or as a continuing review of select critical software components or processes

IV&V Process Overview



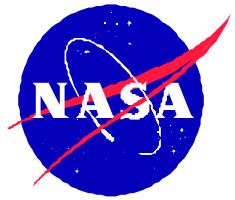
- Project Manager evaluates their project against NASA IV&V Criteria
  - Developed for the NASA Chief Engineer by the NASA Software Working Group
  - Categorizes projects by Likelihood of Failure due to software and the consequences of a failure
  - Evaluation is performed via an online web-based tool
  - Each project receives its own individual URL
    - Contact Ken Costello (Ken.Costello@ivv.nasa.gov) with a Point of Contact with email address and project name
    - POC will receive email in return with project specific URL
    - Questions about filling out the online form can be directed to Ken Costello 3043678343
- Shortly after the PM completes the criteria form, the NASA IV&V Facility will review the results and develop a baseline cost estimate
  - IV&V Facility evaluates results to insure proper interpretation of the criteria
  - Sometimes additional information is required, such as mission goals, proposed organization, instrument information, and software architecture, etc. if available
- The IV&V Facility contacts the project to discuss the results and reach mutual agreement
- Once agreement is reached the IV&V Facility can provide a rough cost estimate
  - Based on general guidelines used during proposal process
  - May be refined based on results of self-assessment

IV&V Process (After Selection)



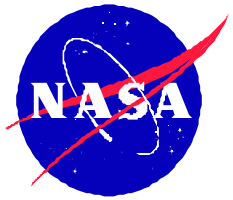
- The project would be asked to at a minimum review the criteria to ensure that nothing has changed
- IV&V Facility personnel work jointly with the program/project office and SMA personnel assigned to the project, to develop a tailored approach to performing the appropriate independent analysis for the project
  - IV&V Facility and program/project management execute MOA to perform a criticality analysis and risk assessment (CARA)
  - IV&V Facility and program/project management reach agreement on the criticality and risk of the software components
  - IV&V Facility develops independent analysis (IV&V or IA) plan based on the criticality and risk
  - Program/Project manager determines whether or not to the pursue the independent analysis indicated by the CARA and documents the decision
- The independent analysis documented in the project plan is subject to IV&V Facility review
  - The program/project's Governing Program Management Council (GPMC) is responsible for approving the program/project's independent analysis approach
- When IV&V or IA is to be performed, the IV&V Facility will determine the distribution of resources between the program/project's development sites and the IV&V Facility
  - The IV&V Facility is responsible for the management of the IV&V work
  - The IV&V Facility manages the resources and the tasking in accordance with the criticality and risks identified in the CFL
- When the project undergoes significant changes that impact the software, the project manager must revisit the criteria
- IV&V, when performed, covers all phases of the software development lifecycle

Appropriate Level of IV&V



- Objective: To confidently support a decision to deploy the system, the following IV&V tasks are required:
  - Requirements, design, code and testing analysis for mission or safety critical functions (failure of function has unacceptable potential to jeopardize mission)
    - Based on Criticality Analysis and Risk Assessment (CARA) score
    - Less critical functions receive a lower level of IV&V effort
    - CARA interpretation is tailored to specific project attributes
    - Should include all software components of the project (flight, ground, instrument, etc.)
  - System level analysis of the integrated system testing plans and their results
  - Continuity of IV&V staffing through the software development life cycle to assure mission requirements and system designs (defined or implicit) are correctly carried forward across phases and organizations
- It is the Facility's intent to be a value added team member, providing the project, GPMC and the Agency an independent assessment of a project's safety or mission critical software and its readiness to deploy
- Facility's satisfactory completion of the appropriate level of IV&V obligates it to support a decision to deploy the system and the liability of that decision

IV&V Costs

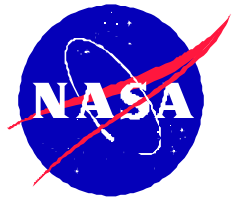


- The cost to do IV&V or IA is directly tied to the perceived risk and criticality of the software
  - Through the analysis performed during the CARA, the risk and criticality of the software components is identified
  - Higher levels of risk and criticality drive more intensive IV&V efforts
    - IV&V Facility and project need to reach a technical agreement on the risk and criticality of the software components
- Earth and Space Science Enterprise Project costs are based on GSA schedule
  - Generally IV&V teams are highly experienced self-directed/motivated people
  - Very little economy of scale as work can not readily be delegated to less experienced employees on small jobs (8 or less FTE)
- Cost also includes Facility overhead charge
  - Facility is not included in GSFC or NASA budget
  - Facility provides its own budget through charging IV&V projects
  - Current charge is 12% (subject to change as more projects are added)
- Indirect Costs
  - There will be interaction between the project and the IV&V Team
  - Interaction is kept to a minimum through participation in project events (i.e. team meetings, PDRs, CDRs, code reviews, etc.)
  - Some need for interaction outside of planned project events to resolve issues

Proposal Baseline

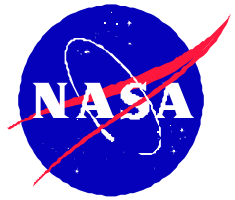
- There are two primary classification for Earth and Space Science Enterprise missions
  - Projects classified as space vehicle (not human-rated), planetary/deep space vehicle, planetary lander or atmospheric vehicle (not human rated)
    - Estimate is 5.5 FTE from three month before implementation phase to four months after delivery
    - 30% of this load is also assumed to be needed from the project start date until 3 months before implementation
    - 40% of this load is also assumed to be needed from four months after delivery until six months after mission is operational
  - Projects classified as space platform (not human-rated) or flight/space instrument
    - Estimate is 3.5 FTE from three month before implementation phase to four months after delivery
    - Other loading is the same as above
- Large projects and human-rated flight missions require generally larger IV&V teams and the cost is determined on a case by case basis
- These base estimates can then be adjusted due to mission unique characteristics (e.g., the Mars 2003 mission has two landers)

IV&V Benefits



- Provides increased confidence that science/project software requirements have been properly implemented
- Provides increased confidence that software requirements verified by analysis or test are completely addressed by the appropriate analysis or test procedure
- Identifies potential instrument/spacecraft software issues prior to I&T
- Increases confidence in the effectiveness of the critical systems, and that those systems have been thoroughly tested
- Provides increased confidence that the software development program is mature and stable, and that late-breaking software issues are handled effectively and are not impacting the effectiveness of the test program
- Provides increased confidence in proceeding to next phase/deployment

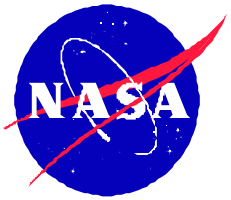
Summary



- NASA policy states that all program/projects with mission and/or safety critical software shall be assessed for IV&V
  - Performed through the self-assessment criteria
  - POC is Ken Costello (ken.costello@ivv.nasa.gov), 3043678343
- Self-assessment results drive cost estimates
  - Based on proposal guidelines
  - Only a rough estimate
  - A more refined estimate is produced after selection
- IV&V Benefits
  - Provides in-depth technical information about the project to the PM
  - Allows the PM to make decisions on risk with information from an objective source
  - Provides developers with unbiased source of help
  - Provides increased confidence in the status of the software development effort

Backup Charts

Criticality Analysis and Risk Assessment



For each Software Component/Function:

Baseline IV&V Analysis Level Thresholds	
IAL	**CARA Score**
None:	**1≤ CARA < 2.5**
Basic:	**2.5 ≤ CARA <4**
Limited:	**4 ≤ CARA < 6**
Focused:	**6 ≤ CARA < 9**
Comprehensive:	**9 ≤ CARA ≤ 12**

Criticality:

Category

- Performance and Operations
- Safety
- Cost/Schedule

Rating

- Catastrophic=4
- Critical=3
- Moderate=2
- Low=1

Average of Criticality Ratings

Risk:

Category

- Complexity
- Technology Maturity
- Reqts Dfn & Stability
- Testability

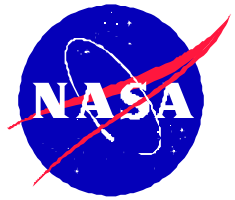
Rating

- High=3
- Moderate=2
- Low=1

Average of Risk Ratings

CARA score

IV&V Analysis Level (IAL)



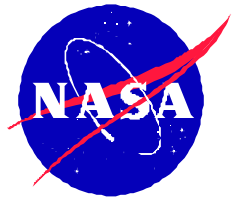
Baseline IALs

- IALs determine the type of tasks to be performed on a given software component/function
- The levels are nominally assigned based on the CARA score

Tailoring IALs

- In almost all cases, the IALs are tailored for the specific project
  - The tailoring allows for a better focusing of IV&V resources
  - Several factors are used in determining the amount of tailoring to include re-use, code size, complexities in the code, mission specific factors, development team skill level and criticality distribution

IV&V Selection Criteria: Consequences of Software Failure



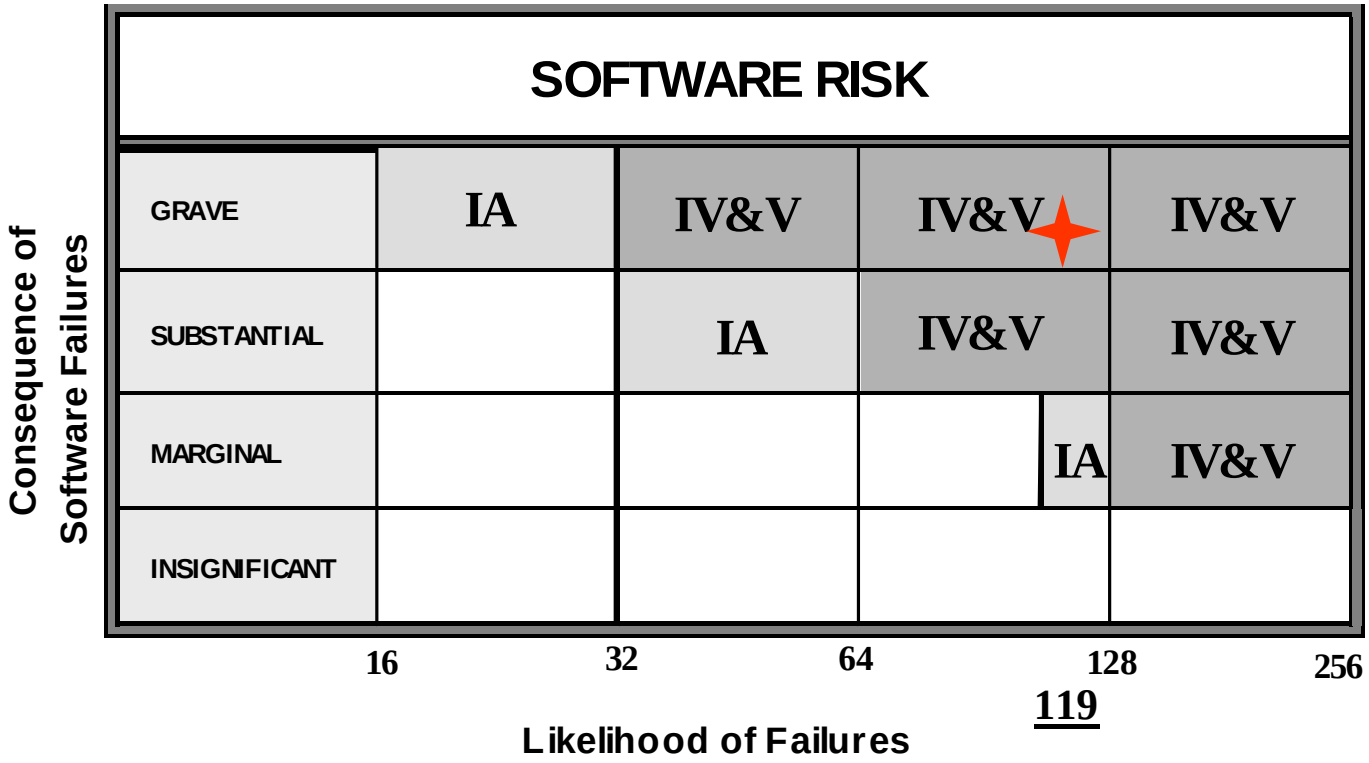
Categories: Grave, Substantial, Marginal, Insignificant

- Potential for loss of life - Yes/No *(Yes = Grave)*
- Potential for serious injury – Yes/No *(Yes = Substantial)*
- Potential for catastrophic mission failure – Yes/No *(Yes = Substantial)*
- Potential for partial mission failure – Yes/No *(Yes = Marginal)*
- **Potential for loss of equipment** – Cost Thresholds
  - *(**$100M = Grave**, $20M = Substantial, $2M = Marginal, < $2M = Insignificant)*
- Potential for waste of resource investment – work year thresholds on software
  - *(>200 = Grave, >100 = Substantial, >20 = Marginal, < 20=Insignificant)*
- Potential for adverse visibility –
  - Center (*Insignificant),* Agency *(Marginal)*, National *(Substantial)*, or International *(Grave)*
- Potential effect on routine operations –
  - Center *(Marginal),* Agency *(Substantial)*

IV&V Selection Criteria: Likelihood of Software Failure

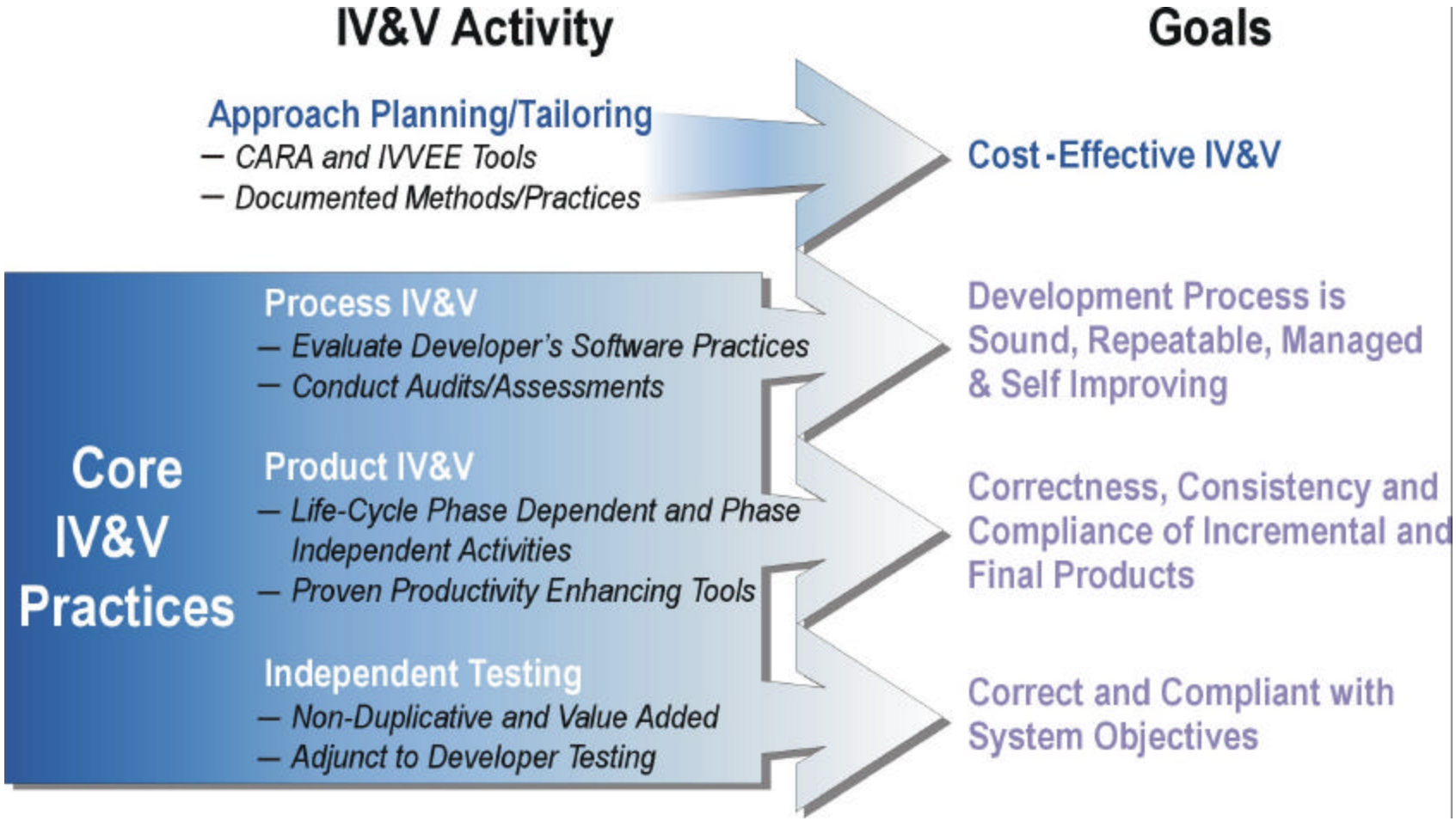
Factors Contributing to probability of software failure	**Un-weighted probability of failure score**					Weighting Factor	Likely-hood of Failure rating
	1	2	4	8	16		
Software Team complexity	Up to 5 people at one location	Up to 10 people at one location	Up to 20 people at one location or 10 people with external support	**Up to 50 people at one location or 20 people with External support**	Up to 50 people at one location or 20 people with External support	X2	16
Contractor Support	None	Contractor with minor tasks		Contractor with major tasks	**Contractor with major tasks critical to project success**	X2	32
Organization Complexity	**One location**	Two locations but same reporting chain	Multiple locations but same reporting chain	Multiple providers with prime sub relationship	Multiple providers with Associate relationship	X1	1
Schedule Pressure	No deadline		Deadline is negotiable	**X**	Non-negotiable deadline	X2	16
Process Maturity of Software Provider	Independent assessment of Capability Maturity Model (CMM) Level 4, 5	Independent assessment of CMM Level 3	Independent assessment of CMM Level 2	**CMM Level 1 with record of Repeated Mission success**	CMM Level 1 or equivalent	X2	16
Degree of Innovation	Proven and accepted	**X**	Proven but new to the Development organization		Cutting edge	X1	2
Level of Integration	Simple - Stand alone			**X**	Extensive Integration Required	X2	16
Requirement Maturity	Well defined objectives - No unknowns	Well defined objectives - Few unknowns		**Preliminary objectives**	Changing, ambiguous, or Untestable objectives	X2	16
Software Lines of Code	Less than 50K	**X**	Over 500K		Over 1000K	X2	4

IV&V Self-Assessment Example

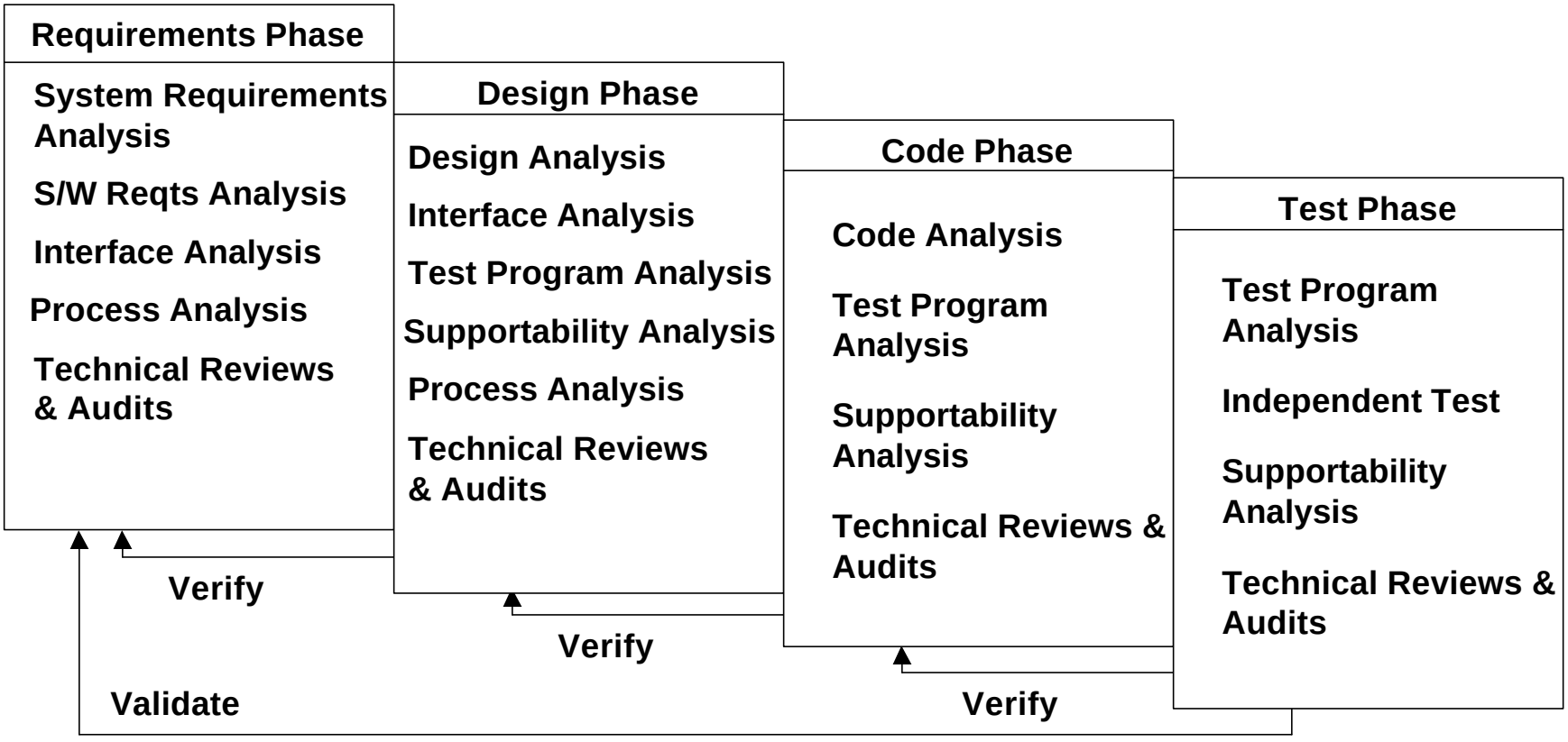


Factors Contributing To Probability of Failure - Example Scoring								
Software Team Complexity	Contractor	Organization Complexity	Schedule Pressure	Process Maturity	Degree of Innovation	Interdepen-dencies of Deliverables	Requirement Clarity	Software Lines of Code
16	32	1	16	16	2	16	16	4

Integrated IV&V Processes Mitigate Risks



IV&V Activities Throughout Lifecycle



Iterative IV&V Methods Promote Efficiency